KNOWLEDGE BASE ARTICLE

# How to Check the Integrity of the Acknowledgement Log

2026 © Vitextra SIA. All rights reserved.

# Disclaimer

For the purposes of this Disclaimer:

- **Company** (referred to as either "the Company", "We", "Us" or "Our" in this Disclaimer) refers to Vitextra SIA, LV-1009 Riga, Matise iela 61 - 25.
- **Document** refers to the Knowledgebase Article.
- **You** means the individual accessing the Document, or the company, or other legal entity on behalf of which such individual is accessing or using the Document, as applicable.
- **Website** refers to Vitextra, accessible from https://vitextra.com

## Disclaimer

The information contained in the Document is for general information purposes only.

The Company assumes no responsibility for errors or omissions in the contents of the Document.

In no event shall the Company be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an action of contract, negligence, or other torts, arising out of or in connection with the use of the contents of the Document. The Company reserves the right to make additions, deletions, or modifications to the contents in the Document at any time without prior notice.

## Errors and Omissions Disclaimer

The information given by the Document is for general guidance on matters of interest only. Therefore, errors can occur even if the Company takes every precaution to ensure that the Document's content is current and accurate. Plus, given the changing nature of laws, rules, and regulations, there may be delays, omissions, or inaccuracies in the information contained in the Document.

The Company is not responsible for any errors or omissions, or for the results obtained from the use of this information.

## Fair Use Disclaimer

The Company may use copyrighted material that the copyright owner has not explicitly authorized. The Company is making such material available for criticism, comment, news reporting, teaching, scholarship, or research.

The Company believes this constitutes a "fair use" of any such copyrighted material as provided for in section 107 of the United States Copyright law.

If You wish to use copyrighted material from the Document for your own purposes that go beyond fair use, You must obtain permission from the copyright owner.

## "Use at Your Own Risk" Disclaimer

All information in the Document is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The Company will not be liable to You or anyone else for any decision made or action taken in reliance on the information given by the Service or for any consequential, special or similar damages, even if advised of the possibility of such damages.

## Contact Us

If you have any questions about this Disclaimer, You can contact Us by email: support@vitextra.com.

# Table of contents

**Prepare the check** 4

**Run verification** 4

**Interpret the result** 4

**Understand the protection limits** 5

**Investigate a failure** 5

The integrity check recomputes hashes for the acknowledgement records and verifies their links to preceding records. It can help detect inconsistencies in the loaded evidence chain. It does not establish that every required event exists, that an employee understood a policy or that the live source still matches a published version.

## Prepare the check

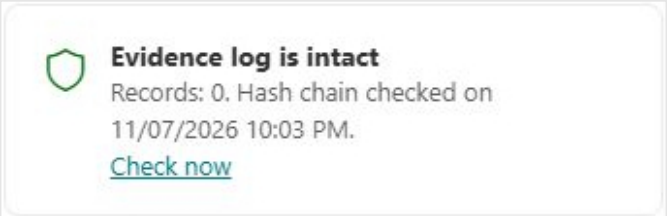
Use an administrator account that can read the acknowledgement list and update product settings and the audit log. The dashboard may be visible to an auditor, but the check saves its result and writes an audit event; read-only access can therefore cause an error after the records have been examined.

If you are investigating suspected damage, preserve the relevant records and identifiers before making changes. Avoid editing evidence, resetting hashes or deleting records as a way to obtain a green result. Coordinate the check with the owner of any service that writes confirmations.

## Run verification

1 Open Compliance Dashboard on the intended hub.
2 Locate the evidence-integrity panel.
3 Review the last saved result, record count and check time. An old result is not a live guarantee for newly added records.
4 Select **Check now** and wait for the operation to finish.
5 Record the new result and timestamp, including the first damaged-record identifier if one is reported.

The check loads the acknowledgement log in ascending record-ID order. It recomputes each record's hash and compares the stored previous-hash link with the preceding record's hash. It concerns the log on that hub, not only the department or policy currently displayed by the dashboard filters.




*Inspecting a saved integrity-check result*

## Interpret the result

| Result | Meaning |
| --- | --- |
| Not verified | No saved verification result is available. |
| Intact | The records loaded for this check had matching hashes and preceding links. |
| Failed | A hash or previous-link mismatch was found; the first affected record is identified. |
| Operation error | The read, calculation or result-saving operation failed; do not treat it as a completed clean check. |

The displayed record count is the loaded log size. When the loop stops at the first mismatch, that number should not be read as proof that every later record was individually validated. An empty log can pass the consistency calculation without proving that any acknowledgement exists.

## Understand the protection limits

The chain can reveal a changed record or a missing middle record whose successor still points to it. Without an independently retained trusted endpoint, removing a suffix of the log or replacing a whole chain is not necessarily detectable by this comparison alone. Concurrent direct writes can also create chain inconsistencies that need investigation rather than an immediate assumption of malicious editing.

**Warning**

The UI's brief wording about proving that no record was changed or removed is broader than this check guarantees. A green result is chain consistency for the loaded data, not absolute immutability, completeness, legal validity or proof of exact source content shown to an employee. Effective permissions and recording mode remain essential; see KB10509. Policy Acknowledgement Data Storage: Direct and Service Modes.

## Investigate a failure

Preserve the first reported record ID, previous record, hashes, check time and recent workflow activity. Inspect related audit events and any service errors with an

administrator. Do not repair the chain by manually replacing stored hashes. If the cause is uncertain, provide support with identifiers and sanitized error details, and keep the original evidence available for investigation. See KB10538. Troubleshooting Failed Acknowledgements and Missing Notifications for recording failures that can leave partial records.